FORM-PTO-1390 (Rev. 12-29-99) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

# TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: 032326-123

U.S. APPLICATION NO (If known, see 37 C F R 1.5): Unassigned 09/763158

| INTERNATIONAL APPLICATION NO. | INTERNATIONAL FILING DATE | PRIORITY DATE CLAIMED |
|---|---|---|
| PCT/FR99/01996 | 16 August 1999 | 17 August 1998 |

TITLE OF INVENTION: METHOD FOR TESTING A RANDOM NUMBER SOURCE AND ELECTRONIC DEVICES COMPRISING SAID METHOD

APPLICANT(S) FOR DO/EO/US: Jean-Sébastien and David NACCACHE

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and the PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

**Items 11. to 16. below concern other document(s) or information included:**

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☐ Other items or information:

| U.S. APPLICATION NO. (If known,/ see 37 C.F.R. 1.5a) | INTERNATIONAL APPLICATION NO | ATTORNEY'S DOCKET NUMBER |
|---|---|---|
| Unassigned 09/763158 | PCT/FR99/01995 | 032326-123 |

| 17. ☒ The following fees are submitted: | CALCULATIONS | PTO USE ONLY |
|---|---|---|
| **Basic National Fee (37 CFR 1.492(a)(1)-(5)):** | | |
| Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO ..... $1,000.00 (960) | | |
| International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO ..... $860.00 (970) | | |
| International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO ..... $710.00 (958) | | |
| International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) ..... $690.00 (956) | | |
| International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) ..... $100.00 (962) | | |
| **ENTER APPROPRIATE BASIC FEE AMOUNT =** | $ 860.00 | |
| Surcharge of **$130.00 (154)** for furnishing the oath or declaration later than 20 ☐ 30 ☐ months from the earliest claimed priority date (37 CFR 1.492(e)). | $ -0- | |

| Claims | Number Filed | Number Extra | Rate | | |
|---|---|---|---|---|---|
| Total Claims | 10 -20 = | -0- | X$18.00 (966) | $ -0- | |
| Independent Claims | 1 -3 = | -0- | X$80.00 (964) | $ -0- | |
| Multiple dependent claim(s) (if applicable) | | | +$270.00 (968) | $ -0- | |
| | | | **TOTAL OF ABOVE CALCULATIONS =** | $ 860.00 | |
| Reduction for 1/2 for filing by small entity, if applicable (see below). | | | | $ -0- | - |
| | | | **SUBTOTAL =** | $ 860.00 | |
| Processing fee of **$130.00 (156)** for furnishing the English translation later than 20 ☐ 30 ☐ months from the earliest claimed priority date (37 CFR 1.492(f)). | | | + | $ -0- | |
| | | | **TOTAL NATIONAL FEE =** | $ 860.00 | |
| Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00 (581)** per property + | | | | $ -0- | |
| | | | **TOTAL FEES ENCLOSED =** | $ 860.00 | |
| | | | **Amount to be: refunded** | $ | |
| | | | **charged** | $ | |

a. ☐ Small entity status is hereby claimed.

b. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

c. ☒ Please charge my Deposit Account No. 02-4800 in the amount of $ 860.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

d. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 02-4800. A duplicate copy of this sheet is enclosed.

**NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.**

SEND ALL CORRESPONDENCE TO:

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

SIGNATURE

James A. LaBarre
NAME

28,632
REGISTRATION NUMBER

Patent
Attorney's Docket No. 032326-123

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | | |
|---|---|---|
| In re Patent Application of | ) | |
| | ) | |
| Jean-Sébastien CORON et al | ) | Group Art Unit: Unassigned |
| | ) | |
| Application No.: Unassigned | ) | Examiner: Unassigned |
| | ) | |
| Filed: February 16, 2001 | ) | |
| | ) | |
| For: METHOD FOR TESTING A RANDOM NUMBER SOURCE AND ELECTRONIC DEVICES COMPRISING SAID METHOD | ) | |



**PRELIMINARY AMENDMENT**

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to examination and the calculation of filing fees, kindly amend the above-identified application as follows:

**IN THE SPECIFICATION**:

Page 1, between lines 2 and 3, insert --This disclosure is based upon, and claims priority from, French Application No. 98/10592 and International Application No. PCT/FR99/01996, the contents of which are incorporated herein by reference.--

**IN THE CLAIMS**:

Claim 7, lines 8-9, replace "any one of Claims 1 to 3" with --Claim 1--.

Claim 10, lines 1-2, replace "any one of Claims 1 to 6" with --Claim 1--.

## REMARKS

Entry of the foregoing amendment is respectfully requested. This amendment is intended to eliminate the multiple dependency of the claims.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: _____

James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: February 16, 2001

Patent
Attorney's Docket No. 032326-123

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | | |
|---|---|---|
| In re Patent Application of | ) | |
| | ) | |
| Jean-Sébastien CORON et al | ) | Group Art Unit: Unassigned |
| | ) | |
| Application No.: 09/763,158 | ) | Examiner: Unassigned |
| | ) | |
| Filed: February 16, 2001 | ) | |
| | ) | |
| For: METHOD FOR TESTING A RANDOM NUMBER SOURCE AND ELECTRONIC DEVICES COMPRISING SAID METHOD | ) | |



**SECOND PRELIMINARY AMENDMENT**

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Kindly amend the above-identified application as follows:

**IN THE SPECIFICATION**:

Page 1, delete the paragraph immediately following the title (which was added in the Preliminary Amendment filed February 16, 2001), and replace it with the following:

--This disclosure is based upon, and claims priority from, French Application No. 98/10592 and International Application No. PCT/FR99/01996, published by the International Bureau on February 24, 2000 in a language other than English, the contents of which are incorporated herein by reference.--

## REMARKS

The foregoing amendment is being made to comply with the new provisions of 37 C.F.R. §1.78(a)(2).

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: _____

James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: April 3, 2001

**Attachment to Second Preliminary Amendment dated April 3, 2001**

**Marked-up Copy**

Page 1, Paragraph Beginning immediately following the title:

--This disclosure is based upon, and claims priority from, French Application No. 98/10592 and International Application No. PCT/FR99/01996, published by the International Bureau on February 24, 2000 in a language other than English, the contents of which are incorporated herein by reference.--

# METHOD FOR TESTING A RANDOM NUMBER SOURCE AND ELECTRONIC DEVICES COMPRISING SAID METHOD

The invention relates to a method for testing sources generating random numbers, in particular sources developed in the context of cryptographic systems such as the random number generators incorporated in chip cards.

It is particularly designed to be used in the testing and validation of electronic devices such as chip cards, PCMCIAs, badges, contactless cards or any other portable apparatus.

The majority of cryptography systems of the public key type (also referred to as asymmetric cryptography) and secret key type (also referred to symmetrical cryptography) require the drawing of secret random values. It is essential that such random values, or numbers, designed to serve as keys subsequently, should a priori be unpredictable and should not exhibit any regularities making it possible to find them by

strategies of exhaustive or enhanced exhaustive search, in which the most probable keys are sought first.

In this regard, there are several methods for testing the random values generated by a random source and to ensure that the said source functions correctly and does not exhibit any drift following changes in external parameters of malevolent origin, such as alteration by induced radiation.

Each of these methods applies to a series, also referred to as a sequence, of integer numbers between 0 and a value d, the said series being generated by the random source.

The most widely known test method is the so-called "frequency" test. It is a case of counting the number of appearances of each integer between 0 and a value d in the said sequence. The number of appearances of each integer is then evaluated statistically.

A second so-called "series" test method consists in a counting and statistical evaluation of the number of appearances of all the possible pairs of integers between 0 and a value d. This test method can be broadened to the counting of triplets or quadruplets of integers, etc.

A third so-called "hole" test method exists. A hole in a sequence is a series of numbers outside a predetermined interval. It is a case of a statistical evaluation of the length of the said holes in the sequence.

A fourth test method, known as the "poker" test, exist. The test consists in grouping together the

numbers in the sequence in groups of five numbers and counting in each quintuplet how many different values appear.

A fifth test method, known as the "collection of coupons", consists of statistically evaluating the sequence size necessary for all the integer values between 0 and d to appear in the said sequence.

The details of these methods are found in the work by Knuth, entitled "The Art of Computer Programming, Vol. 2, Seminumerical Algorithms".

Another popular test method is Maurer's universal test described in the work "Journal of Cryptography", Vol. 5, N° 2, 1992, pp 89-105. This test has the advantage of revealing all the faults detectable by the test methods previously cited as well as other statistical defects not detected by these same test methods.

The so-called Maurer test method, also referred to as the universal method, comprises the following steps:

Step one: Generation of a sequence of (Q+K)*L bits by the random source. Q, K and L are input parameters. The bits in the sequence are grouped in blocks of L bits, forming a sequence of integers between 0 and $2^L$-1 of length Q+K. The length is stored in the table block[n], where n is between 1 and Q+K.

Step two: Calculating the test parameter, denoted fTU; this second step comprising the following steps, referred to as substeps 2.1 to 2.5:

2.1 Creation and initialisation of a table tab[i] of size $2^L$;

2.2 For n varying from 1 to Q, making the calculation: tab[block[n]]=n;

2.3 Initialising the number Sum to 0;

2.4 For n varying from Q+1 to Q+K, performing the calculation:

Add log(n-tab[block[n]] to Sum;

Make the calculation: tab[block[n]]=n;

2.5 The parameter fTU of the test is given by:

fTU=(Sum/K)/Log(2);

Step three: Calculation of the variance per test parameter block, denoted Var. Its precise expression is given in the article published by Maurer in the work "Journal of Cryptography", Vol 5, N° 2, 1992, pp. 89-105, which is:

$$Var = (1 - z) * \sum_{i=1}^{\infty} \log 2(i)^2 * z^{i-1} - ((1 - z) * \sum_{i=1}^{\infty} \log 2(i) * z^{i-1})^2$$

with log2(z)=log(z)/log(2) and $z=1-2^{-L}$

Step four: Calculation of the function c(L,K). An approximate expression of this function is given in the article in the abovementioned work, which is:

C(L,K)=0.7-0.8/L+(1.6+12.8/L)*K(-4/L);

Step five: Calculation of the standard deviation of the test parameter, denoted σ: σ=c(L.K)*√(Var/K);

Step six: Calculation of the parameter y; y is determined from the rejection rate of the test fixed as an input, denoted ρ. Y must satisfy the equation:

N(-y)=ρ.

N is the normal density function described in the work by R. Langley: "Practical Statistics", Dover publications, New York, 1968. The equation N(-y)=ρ can

be resolved using a table of values of N. Such a table is supplied in the abovementioned article.

Step seven: Calculation of the ideal mean value of the test, denoted E[fTU]. Its expression is given in the article published by Maurer in the work "Journal of Cryptography", Vol 5, N° 2, 1992, pp. 89-105, and is equal to:

$$E[fTU] = (1 - z) * \sum_{i=1}^{n} \log 2(i) * z^{i-1}$$

with $\log 2(z) = \log(z)/\log(2)$ and $z = 1 - 2^{-L}$

Step eight: Calculation of the bounds t1 and t2. They are given by the equation: $t1 = E[fTU] - y*\sigma$ and $t2 = E[fTU] + y*\sigma$.

Step nine: Result of the test.

If the test parameter fTU is between t1 and t2, then the random number generator is accepted. In the contrary case, it is refused.

The universal test method is therefore based on an approximation in the calculation of the function c(L,K). This approximation makes the test less precise than is wished by the theoretical guarantee serving as a basis for it. It is possible to show that, in certain cases, the universal test proves to be 2.67 times too permissive compared with what is allowed by theory.

The object of the present invention is an improved test method for achieving the real precision guaranteed by the theoretical analysis of the universal test. This test serves notably to improve the security of portable devices of the chip card type.

The method of the invention consists in replacing step 4 of the universal test by the precise calculation of the function c(L,K). This calculation is based on a probabilistic analysis of the universal test.

The present invention gives three distinct expressions of the function c(L,K), according to the values of the parameters L and K.

The first expression of c(L,K) is valid whatever the parameters L and K.

The second expression of c(L,K) is valid in the case where the value L is between 3 and 16 and the value K is greater than $30*2^L$, which corresponds to the most usual case of use of the test. It is much more simple to calculate than the first expression and can therefore be effected on a simple microcontroller in a few milliseconds.

The third expression of c(L,K) is valid for a value of L>16 and a value of $K>30*2^L$. This expression is even more simple to calculate.

The first expression of c(L,K) can be obtained by means of the method described below, which contains nine steps:

1. Calculation of: $u=1-2^{-L}$ and $v=1-1/(2^L-1)$;
u and v being real numbers;

2. Creation of two tables tab1 and tab2 of size $60*2^L$;

3. Filling of tab1 and tab2: for this purpose,

3.1 Execute z=u, sum=0, z1=1;

3.2 For i ranging from 1 to $30*2^L$, repeating the two operations which are: add log2(i)*z1 to sum, in which log2 designates the logarithm to base 2, and

calculate: z1=z1*z;

3.3 Execute tab1[0]=(1-z)*sum;

3.4 For i ranging from 1 to $60*2^L$,

Execute tab1[i]=(tab1[i-1]-(1-z)*log2(i))/z;

3.5 Repeat steps 3.1, 3.2, 3.3, 3.4, replacing u with v and tab1 with tab2;

4. Calculation of the variance per block denoted Var;

4.1 Execute sum=0 and x=1;

4.2 For i varying from 1 to $30*2^L$, execute the following two operations:

Add $\log2(i)^2*x$ to sum and

Execute x=x*z;

4.3 Make Var=$sum/2^L-tab1[0]^2$;

5. Calculation of P(K);

5.1 Make sum=0 and x=1;

5.2 For i varying from 1 to $30*2^L$: carry out the following three operations:

Calculate y:$y=u^2*(tab2[i+K-1]-tab1[i+K])*(tab2[0]-v^i*tab2[i])+u*tab1[0]*(tab1[i+K-1]-tab2[i+K-1])$,

Add y*x to sum,

Execute x=x*u;

5.3 Execute $P(K)=u^{(K-1)}*sum$;

6. Calculation of P(1):

Same method as at step 5, replacing K with 1;

7. Calculation of Q(K):

7.1 Make sum=0, sum2=0 and x=1,

7.2 For i varying from 1 to $30*2^{\wedge}L$:

Add $i*\log2(i)*u^{(i-2)}$ to sum2;

Execute the following three operations:

Calculate $y=u^2*(tab2[i+K-1]-tab1[i+K])*((i+k)*tab2[0]-v^i*tab2[i])-2^{(-L)}*sum2)+u*(i+K-1)*tab1[0]*(tab1[i+K-1]-tab2[i+K=1])$,

Add y*x to sum,

Execute x=x*u;

7.3 Execute $Q(K)=u^{(K-1)}*sum$

8. Calculation of Q(1)

Same method as at step 7, replacing K with 1

9. Calculation of c(L,K)

$c(L,K)=\sqrt{(1-2/Var*(P(1)-P(K)-(Q(1)-Q(K))/K)}$

The second expression of c(L,K) is valid for $K>30*2^L$. It is calculated according to the following method in two steps:

Step one: Reading of the values of e(L) and d(L), e and d being real values, listed in the following table, for L between 3 and 16:

| L | d(L) | e(L) |
|---|---|---|
| 3 | 0.2732725 | 0.4890883 |
| 4 | 0.3045101 | 0.4435381 |
| 5 | 0.3296587 | 0.4137196 |
| 6 | 0.3489769 | 0.3941338 |
| 7 | 0.3631815 | 0.3813210 |
| 8 | 0.3732189 | 0.3730195 |
| 9 | 0.3800637 | 0.3677118 |
| 10 | 0.3845867 | 0.3643695 |
| 11 | 0.3874942 | 0.3622979 |

| | | |
|---|---|---|
| 12 | 0.3893189 | 0.3610336 |
| 13 | 0.3904405 | 0.3602731 |
| 14 | 0.3911178 | 0.3598216 |
| 15 | 0.3915202 | 0.3595571 |
| 16 | 0.3917561 | 0.3594040 |

Step two: Calculate the value $c(L,K)$ using the formula:

$$c(L,K)=\sqrt{(d(L)+e(L)*2^L/K)}$$

The third expression of $c(L,K)$ is valid for $L>16$ and $K>30*2^L$. It is given by the following formula:

$$c(L,K)=\sqrt{(1-6/\Pi^2+2/\Pi^2*(4*\log(2)-1)*2^L/K)}$$

The present invention also relates , as stated at the beginning of the description, page 1, to an electronic device which is not depicted by a figure or diagram. This electronic device is a device for the automatic verification of the physical integrity of a self-checking integrated circuit checking the integrity of its random generator from the three variants of the method of the invention, also described above, or more explicitly from the three distinct expressions of the function $c(L,K)$, in order to ensure that the said generator is functioning correctly in general and does not exhibit any drift following changes in external parameters of malevolent origin, such as an alteration by induced radiation, in particular.

Preferentially, the electronic device carrying out the test is a portable device, and more particularly consists, for example, of a chip card, a contactless card, a PCMCIA card, a badge or an intelligent watch.

Finally, the electronic device of the invention can be an external device consisting of a machine or installation designed to test the correct functioning of random generators incorporated in the said portable devices. This external device allows an exchange of information with the portable device so as to check that the random generator is functioning correctly. The external device interacts with the portable device in order to check the integrity of its random generator.

## CLAIMS

1. A method for testing sources of random numbers, comprising the following steps:

Step one: Generation of a sequence of (Q+K)*L bits by the random source, Q, K and L being input parameters, the bits in the sequence being grouped in blocks of L bits, forming a sequence of integers between 0 and $2^L$-1 of length Q+K, the length being stored in the table block[n], where n is between 1 and Q+K;

Step two: Calculating the test parameter, denoted fTU; this second step comprising the following steps, referred to as substeps 2.1 to 2.5:

2.1 Creation and initialisation of a table tab[i] of size $2^L$;

2.2 For n varying from 1 to Q, making the calculation: tab[block[n]]=n;

2.3 Initialising the number Sum to 0;

2.4 For n varying from Q+1 to Q+K, performing the calculation in two operations:

Add log(n-tab[block[n]] to Sum;

Make the calculation: tab[block[n]]=n;

2.5 The parameter fTU of the test is given by:

fTU=(Sum/K)/Log(2);

Step three: Calculation of the variance per test parameter block, denoted Var, from the following expression:

$$Var = (1 - z) * \sum_{i=1}^{\infty} \log 2(i)^2 * z^{i-1} - ((1 - z) * \sum_{i=2}^{\infty} \log 2(i) * z^{i-1})^2$$

with $\log2(z)=\log(z)/\log(2)$ and $z=1-2^{-L}$

Step four: Calculation of the function c(L,K);

Step five: Calculation of the standard deviation of the test parameter, denoted σ: $\sigma=c(L.K)*\sqrt{(Var/K)}$;

Step six: Calculation of the parameter y; y is determined from the rejection rate of the test fixed as an input, denoted ρ. Y must satisfy the equation:

$N(-y)=\rho$,

N is the normal density function;

Step seven: Calculation of the ideal mean value of the test, denoted E[fTU], given by the following formula:

$$E[fTU] = (1 - z) * \sum_{i=1}^{\infty} \log 2(i) * z^{i-1}$$

with $\log2(z)=\log(z)/\log(2)$ and $z=1-2^{-L}$

Step eight: Calculation of the bounds t1 and t2. They are given by the equation: $t1=E[fTU]-y*\sigma$ and $t2=E[fTU]+y*\sigma$;

Step nine: Result of the test: the random number generator being accepted if the test parameter fTU is between t1 and t2, and rejected in the contrary case,

the said method being characterised in that step four consists of a calculation of the function c(L,K) which is valid whatever the parameters L and K.

2. A method for testing sources of random numbers according to Claim 1, characterised in that step four consists of a calculation of the function c(L,K) which is valid in the case where the value of L is between 3 and 16 and the value of K is greater than $30*2^{L}$.

3. A method for testing sources of random numbers according to Claim 1, characterised in that step four consists of a calculation of the function c(L,K) which is valid for a value of L>16 and a value of $K>30*2^L$.

4. A method according to Claim 1, characterised in that the calculation of the function c(L,K) contains nine steps:

1. Calculation of: $u=1-2^{-L}$ and $v=1-1/(2^L-1)$;

u and v being real numbers;

2. Creation of two tables tab1 and tab2 of size $60*2^L$;

3.1 Execute z=u, sum=0, z1=1;

3.2 For i ranging from 1 to $30*2^L$, repeating the two operations which are: add log2(i)*z1 to sum, in which log2 designates the logarithm to base 2, and

calculate: z1=z1*z;

3.3 Execute tab1[0]=(1-z)*sum;

3.4 For i ranging from 1 to $60*2^L$,

Execute tab1[i]=(tab1[i-1]-(1-z)*log2(i))/z;

3.5 Repeat steps 3.1, 3.2, 3.3, 3.4, replacing u with v and tab1 with tab2;

4. Calculation of the variance per block denoted Var;

4.1 Execute sum=0 and x=1;

4.2 For i varying from 1 to $30*2^L$, execute the following two operations:

Add $\log2(i)^2*x$ to sum and

Execute x=x*z;

4.3 Make $Var=sum/2^L-tab1[0]^2$;

5. Calculation of P(K);

5.1 Make sum=0 and x=1;

5.2 For i varying from 1 to $30*2^L$: carry out the following three operations:

Calculate y:$y=u^2*(tab2[i+K-1]-tab1[i+K])*(tab2[0]-v^i*tab2[i])+u*tab1[0]*(tab1[i+K-1]-tab2[i+K-1])$,

Add y*x to sum,

Execute x=x*u;

5.3 Execute $P(K)=u^{(K-1)}*sum$;

6. Calculation of P(1):

Same method as at step 5, replacing K with 1;

7. Calculation of Q(K):

7.1 Make sum=0, sum2=0 and x=1,

7.2 For i varying from 1 to 30*2^L:

Add $i*\log2(i)*u^{(i-2)}$ to sum2;

Execute the following three operations:

Calculate $y=u^2*(tab2[i+K-1]-tab1[i+K])*((i+k)*tab2[0]-v^i*tab2[i])-2^{(-L)}*sum2)+u*(i+K-1)*tab1[0]*(tab1[i+K-1]-tab2[i+K=1])$,

Add y*x to sum,

Execute x=x*u;

7.3 Execute $Q(K)=u^{(K-1)}*sum$

8. Calculation of Q(1)

Same method as at step 7, replacing K with 1

9. Calculation of c(L,K)

$c(L,K)=\sqrt{(1-2/Var*(P(1)-P(K)-(Q(1)-Q(K))/K)}$

5. A method according to Claim 2, characterised in that the function c(L,K) contains two steps:

Step one: Reading of the values of e(L) and d(L), e and d being real values, listed in the following table, for L between 3 and 16:

| L | d(L) | e(L) |
|---|---|---|
| 3 | 0.2732725 | 0.4890883 |
| 4 | 0.3045101 | 0.4435381 |
| 5 | 0.3296587 | 0.4137196 |
| 6 | 0.3489769 | 0.3941338 |
| 7 | 0.3631815 | 0.3813210 |
| 8 | 0.3732189 | 0.3730195 |
| 9 | 0.3800637 | 0.3677118 |
| 10 | 0.3845867 | 0.3643695 |
| 11 | 0.3874942 | 0.3622979 |
| 12 | 0.3893189 | 0.3610336 |
| 13 | 0.3904405 | 0.3602731 |
| 14 | 0.3911178 | 0.3598216 |
| 15 | 0.3915202 | 0.3595571 |
| 16 | 0.3917561 | 0.3594040 |

Step two: Calculate the value c(L,K) using the formula:

$$c(L,K) = \sqrt{(d(L) + e(L) * 2^L / K)}$$

6. A method according to Claim 3, characterised in that the calculation of the functions c(L,K) is effected by means of the following formula:

$$c(L,K) = \sqrt{(1 - 6/\Pi^2 + 2/\Pi^2 * (4 * \log(2) - 1) * 2^L / K)}$$

7. An electronic device for the self-checking of the physical integrity of a self-checking integrated circuit and checking the integrity of its random generator, in order to ensure that the latter is functioning correctly in general and does not exhibit any drift following changes in external parameters of

malevolent origin such as an alteration by induced radiation, in particular, according to any one of Claims 1 to 3.

8. An electronic device according to Claim 7, characterised in that the device performing the test is a portable device.

9. An electronic device according to Claim 8, characterised in that the device is a chip card, a contactless card, a PCMCIA card, a badge or an intelligent watch.

10. An electronic device according to any one of Claims 1 to 6, characterised in that an external device performing the test consists of a machine or installation designed to test the correct functioning of random generators incorporated in the said portable devices.

| COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY<br>(Includes Reference to Provisional and PCT International Applications) | Attorney's Docket No.<br>032326-123 |
|---|---|



As a below named inventor, I hereby declare that:
My residence, post office address and citizenship are as stated below next to my name;
I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD FOR TESTING A RANDOM NUMBER SOURCE AND ELECTRONIC DEVICES COMPRISING SAID METHOD

the specification of which (check only one item below):

☐ is attached hereto.

☒ was filed as United States application
Number 09/763,158
on February 16, 2001
and was amended
on _____ (if applicable).

☐ was filed as PCT international application
Number _____
on _____
and was amended
on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 (a)-(e) of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. §119:

| COUNTRY<br>(if PCT, indicate "PCT") | APPLICATION NUMBER | DATE OF FILING<br>(day, month, year) | PRIORITY CLAIMED<br>UNDER 35 U.S.C. §119 |
|---|---|---|---|
| France | 98/10592 | 17 August 1998 | X Yes _No |
| | | | _Yes _No |
| | | | _Yes _No |
| | | | _Yes _No |
| | | | _Yes _No |

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

_____ _____
(Application Number) (Filing Date)

_____ _____
(Application Number) (Filing Date)

| COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONT'D)<br>(Includes Reference to Provisional and PCT International Applications) | Attorney's Docket No.<br>032326-123 |
|---|---|

I hereby claim the benefit under Title 35, United States Code, §120 of any United States applications(s) or PCT international application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose to the Office all information known to me to be material to the patentability as defined in Title 37, Code of Federal Regulations §1.56, which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

PRIOR U.S. APPLICATIONS OR PCT INTERNATIONAL APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. §120:

| U.S. APPLICATIONS | | STATUS *(check one)* | | |
|---|---|---|---|---|
| U.S. APPLICATION NUMBER | U.S. FILING DATE | PATENTED | PENDING | ABANDONED |
| | | | | |
| | | | | |
| | | | | |

| PCT APPLICATIONS DESIGNATING THE U.S. | | | | | |
|---|---|---|---|---|---|
| PCT APPLICATION NO. | PCT FILING DATE | U.S. APPLICATION NUMBERS ASSIGNED (if any) | | | |
| PCT/FR99/01996 | 16 August 1999 | | | | |
| | | | | | |
| | | | | | |

I hereby appoint the following attorneys and agent(s) to prosecute said application and to transact all business in the Patent and Trademark Office connected therewith and to file, prosecute and to transact all business in connection with international applications directed to said invention:

| | | | | | |
|---|---|---|---|---|---|
| William L. Mathis | 17,337 | Eric H. Weisblatt | 30,505 | Bruce T. Wieder | 33,815 |
| Robert S. Swecker | 19,885 | James W. Peterson | 26,057 | Todd R. Walters | 34,040 |
| Platon N. Mandros | 22,124 | Teresa Stanek Rea | 30,427 | Ronni S. Jillions | 31,979 |
| Benton S. Duffett, Jr. | 22,030 | Robert E. Krebs | 25,885 | Harold R. Brown III | 36,341 |
| Norman H. Stepno | 22,716 | William C. Rowland | 30,888 | Allen R. Baum | 36,086 |
| Ronald L. Grudziecki | 24,970 | T. Gene Dillahunty | 25,423 | Steven M. duBois | 35,023 |
| Frederick G. Michaud, Jr. | 26,003 | Patrick C. Keane | 32,858 | Brian P. O'Shaughnessy | 32,747 |
| Alan E. Kopecki | 25,813 | B. Jefferson Boggs, Jr. | 32,344 | Kenneth B. Leffler | 36,075 |
| Regis E. Slutter | 26,999 | William H. Benz | 25,952 | Fred W. Hathaway | 32,236 |
| Samuel C. Miller, III | 27,360 | Peter K. Skiff | 31,917 | Wendi L. Weinstein | 34,456 |
| Robert G. Mukai | 28,531 | Richard J. McGrath | 29,195 | Mary Ann Dillahunty | 34,576 |
| George A. Hovanec, Jr. | 28,223 | Matthew L. Schneider | 32,814 | | |
| James A. LaBarre | 28,632 | Michael G. Savage | 32,596 | | |
| E. Joseph Gess | 28,510 | Gerald F. Swiss | 30,113 | | |
| R. Danny Huntington | 27,903 | Charles F. Wieland III | 33,096 | | |

21839

and: _____

Address all correspondence to:

21839

James A. LaBarre
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404

Address all telephone calls to: James A. LaBarre at (703) 836-6620.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

| COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONT'D)<br>(Includes Reference to Provisional and PCT International Applications) | Attorney's Docket No.<br>032326-123 |
|---|---|

| FULL NAME OF SOLE OR FIRST INVENTOR<br>Jean-Sébastien CORON | SIGNATURE | DATE<br>2/14/07 |
|---|---|---|
| RESIDENCE<br>4 rue Léon de Lagrange, 75015, Paris, FRANCE FRX | CITIZENSHIP<br>France | |
| POST OFFICE ADDRESS<br>4 rue Léon de Lagrange, 75015, Paris, FRANCE | | |
| FULL NAME OF SECOND JOINT INVENTOR, IF ANY<br>David NACCACHE | SIGNATURE<br>David Naccache | DATE<br>2/4/01 |
| RESIDENCE<br>7 rue Chaptal, 75009 Paris, FRANCE FRY | CITIZENSHIP<br>France | |
| POST OFFICE ADDRESS<br>7 rue Chaptal, 75009 Paris, FRANCE | | |
| FULL NAME OF THIRD JOINT INVENTOR, IF ANY | SIGNATURE | DATE |
| RESIDENCE | CITIZENSHIP | |
| POST OFFICE ADDRESS | | |
| FULL NAME OF FOURTH JOINT INVENTOR, IF ANY | SIGNATURE | DATE |
| RESIDENCE | CITIZENSHIP | |
| POST OFFICE ADDRESS | | |
| FULL NAME OF FIFTH JOINT INVENTOR, IF ANY | SIGNATURE | DATE |
| RESIDENCE | CITIZENSHIP | |
| POST OFFICE ADDRESS | | |
| FULL NAME OF SIXTH JOINT INVENTOR, IF ANY | SIGNATURE | DATE |
| RESIDENCE | CITIZENSHIP | |
| POST OFFICE ADDRESS | | |
| FULL NAME OF SEVENTH JOINT INVENTOR, IF ANY | SIGNATURE | DATE |
| RESIDENCE | CITIZENSHIP | |
| POST OFFICE ADDRESS | | |
| FULL NAME OF EIGHTH JOINT INVENTOR, IF ANY | SIGNATURE | DATE |
| RESIDENCE | CITIZENSHIP | |
| POST OFFICE ADDRESS | | |